

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

1 **In the Claims:**

2 Please replace the pending claims 1-57 with those set forth below, in which
3 claims 35, 39, 42-44, 46-48, and 50 are amended and claims 1-34, and 52-57 are
4 canceled without prejudice.

5
6 1-34. (Canceled)

7
8
9 35. (Currently Amended) A home control system that uses
10 electrical power lines for communications, comprising:

11 a plurality of components that are connected for
12 communications among themselves through the electrical power lines, wherein the
13 communications among the plurality of components is established through a single
14 communication protocol;

15
16 a sending one of the components being configured to send
17 messages over the electrical power lines in accordance with [[steps]] acts
18 comprising:

19 calculating a first message authentication code based
20 on a predefined one-way function of data from a message and of a key value that is
21 shared between sending and receiving components;

22 including the message authentication code in the
23 message;
24
25

1 sending the message over the electrical power lines;
2 a receiving one of the components being configured to receive
3 messages in accordance with [[steps]] acts comprising:
4 receiving a message over the electrical power lines;
5 calculating a second message authentication code
6 based on the predefined one-way function of the data from the message and of the
7 a current shared key value;
8 concluding that the message is either not authentic or
9 contains a data error if the first and second message authentication codes do not
10 match.
11
12

13 36. (Original) A home control system as recited in claim 35, wherein
14 the shared key value is from a sequence of key values;

15 the sending component being further configured to change
16 from a current to a subsequent key value in the sequence without notifying the
17 receiving component;
18

19 the receiving component being further configured to calculate
20 a third message authentication code based on the predefined one-way function of
21 the data from the message and of the subsequent key value;
22

23 the receiving being further configured to change from the
24 current key value to the subsequent key value if the first and second message
25

1 authentication codes do not match but the first and third message authentication
2 codes do match.

3
4 37. (Original) A home control system as recited in claim 35, wherein
5 the shared key value is from a sequence of key values;

6 the sending component being further configured to change
7 from a current to a subsequent key value in the sequence without notifying the
8 receiving component;

9 the receiving component being further configured to calculate
10 a third message authentication code based on the predefined one-way function of
11 the data from the message and of the subsequent key value;

12 the receiving being further configured to change from the
13 current key value to the subsequent key value if the first and second message
14 authentication codes do not match but the first and third message authentication
15 codes do match;

16 wherein the sending and receiving components calculate the
17 sequence of key values using a one-way function of a counter value that advances
18 to generate each sequential key value.

19
20
21
22
23 38. (Original) A home control system as recited in claim 35, wherein
24 the shared key value is from a sequence of key values, and wherein the sending
25

1 and receiving components calculate the sequence of key values using a one-way
2 function of counter values that advance to generate each sequential key value.

3
4 39. (Currently Amended) [[A]] An electrical component that is
5 connected for communications with other electrical components of a particular
6 group using electrical power lines in a building, comprising:

7 a processor;

8 a transmitter that is responsive to the processor to send data
9 using the electrical power lines;

10 the processor being programmed to compose and send
11 messages in conjunction with the transmitter, each message including a message
12 authentication code based on a predefined one-way function of data from the
13 message and of a key value that is shared between a plurality of components;

14 wherein the communications with other electrical components
15 of the particular group is established through a single communication protocol.

16
17
18
19 40. (Original) An electrical component as recited in claim 39,
20 wherein the shared key value is from a sequence of key values, the processor being
21 further programmed to change from a current to a subsequent key value in the
22 sequence without notifying a receiving component.
23
24
25

1 41. (Original) An electrical component as recited in claim 39,
2 wherein the shared key value is from a sequence of key values, wherein the
3 processor calculates the sequence of key values using a one-way function of a
4 counter values that advance to generate each sequential key value.

5
6 42. (Currently Amended) [[A]] An electrical component that is
7 connected for communications with other electrical components of a particular
8 group using electrical power lines in a building, comprising:
9

10 a processor;

11 a receiver that functions in conjunction with the processor to
12 receive messages from other electrical components using the electrical power
13 lines, such messages including first message authentication codes;

14 the processor being programmed to calculate a second
15 message authentication code for each message based on a predefined one-way
16 function of the data from the message and of a key value that is shared between a
17 plurality of components;

18 the processor being further programmed to compare the first
19 and second message authentication codes to authenticate each message;
20

21 wherein the communications with other electrical components
22 of the particular group is established through a single communication protocol.
23
24
25

1 43. (Currently Amended) An electrical component as recited in
2 claim 42, wherein the shared key value is from a sequence of key values, the
3 processor programmed to perform the following [[steps]] operations:

4 calculating a third message authentication code based on the
5 predefined one-way function of the data from the message and of a subsequent key
6 value in the sequence of key values;

7 further comparing the first and third message authentication
8 codes to authenticate each message.
9

10 changing from the current key value to the subsequent key
11 value if the first and second message authentication codes do not match but the
12 first and third message authentication codes do match.
13

14
15 44. (Currently Amended) An electrical component as recited in
16 claim 42, wherein the shared key value is from a sequence of key values, the
17 processor programmed to perform the following [[steps]]:

18 calculating the sequence of key values using a one-way
19 function of a counter value that advances to generate each sequential key value;

20 calculating a third message authentication code based on the
21 predefined one-way function of the data from the message and of a subsequent key
22 value in the sequence of key values;
23
24
25

1 further comparing the first and third message authentication
2 codes to authenticate each message [[.]] ;

3 changing from the current key value to the subsequent key
4 value if the first and second message authentication codes do not match but the
5 first and third message authentication codes do match.
6

7
8 45. (Original) An electrical component as recited in claim 42,
9 wherein the shared key value is from a sequence of key values, wherein the
10 processor calculates the sequence of key values using a one-way function of a
11 counter value that advances to generate each sequential key value.
12

13 46. (Currently Amended) A method of communicating
14 electronically between a plurality of electrical components using electrical power
15 lines in a building, the method comprising ~~the following steps~~:
16

17 designating groups of the electrical components that
18 communicate among themselves;

19 sharing a key value between components of a particular
20 group;
21

22 calculating a first message authentication code based on a
23 predefined one-way function of data from a message and of the key value that is
24 shared by components of the particular group;
25

1 including the message authentication code in the message;
2 sending the message over the electrical power lines;
3 receiving the message;
4 calculating a second message authentication code based on
5 the predefined one-way function of the data from the message and of the shared
6 key value; and
7 comparing the first and second message authentication codes
8 to authenticate each message;
9 wherein the electronic communication between the electrical
10 components is established through a single communication protocol.
11

12
13 47. (Currently Amended) A method as recited in claim 46, wherein
14 the shared key value is from a sequence of key values, the method further
15 comprising an additional [[step]] act of changing from a current to a subsequent
16 key value in the sequence without notifying receiving components.
17

18
19 48. (Currently Amended) A method as recited in claim 46, wherein
20 the shared key value is from a sequence of key values, the method further
21 comprising:
22
23
24
25

1 calculating a third message authentication code based on the
2 predefined one-way function of the data from the message and of a subsequent key
3 value in the sequence of key values;

4 further comparing the first and third message authentication
5 codes to authenticate each message [.] ;

6 changing from the current key value to the subsequent key
7 value if the first and second message authentication codes do not match but the
8 first and third message authentication codes do match.
9

10
11 49. (Original) A method as recited in claim 46, wherein the shared
12 key value is from a sequence of key values, the method further comprising:

13 calculating the sequence of key values using a one-way
14 function of a counter value that advances to generate each sequential key value;

15 calculating a third message authentication code based on the
16 predefined one-way function of the data from the message and of a subsequent key
17 value in the sequence of key values;

18 further comparing the first and third message authentication
19 codes to authenticate each message;
20

21 changing from the current key value to the subsequent key
22 value if the first and second message authentication codes do not match but the
23 first and third message authentication codes do match.
24
25

1
2 50. (Currently Amended) A method component as recited in claim
3 46, wherein the shared key value is from a sequence of key values, further
4 comprising ~~a step of~~ calculating the sequence of key values using a one-way
5 function of a counter value that advances to generate each sequential key value.
6

7
8 51. (Original) A method as recited in claim 46, further comprising:
9 assigning different group identifier codes to different groups
10 of components;
11 specifying the group identifier code of an individual group in
12 messages sent to components of said individual group;
13 determining whether a particular message is intended for a
14 particular component by checking whether the group identifier code of the
15 particular message matches the group identifier code of the particular component's
16 group.
17

18
19 52-57. (Canceled)
20
21
22
23
24
25